DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO
ATTENTION OF
IMSW-SMH-IM

11 JUL 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-03, User Responsibilities for Information System Sustainment

1. REFERENCES.

a. DOD Directive 5500-7-R, Joint Ethics Regulation (JER), 30 August 1993.

b. AR 25-2, Information Assurance, 14 November 2003.

c. AR 25-1, Army Knowledge Management and Information Technology , 15 July 2005.

d. FSH Regulation 690-26, Conduct and Discipline, 5 March 1997.

e. Memorandum, MCCS-Z, subject: User Responsibilities for Information Systems Sustainment Policy, 7 January 2002.

f. USAG FSH Policy Statement Number 31, subject: Use of Federal Government Communications Systems and Resources, August 2004.

2. PURPOSE. This policy outlines the responsibilities of the information system user on Fort Sam Houston (FSH), satellite sub-installations, and all other work sites connected to the installation network. This policy assigns responsibilities, and provides guidance in applying information technology best business practices in day-to-day use and protection of information systems.

3. SCOPE. This policy applies to all organizations receiving reimbursable services from the Director of Information Management (DOIM) to the extent of the products and services they use.

4. POLICY. Each of the following policy categories has several components of which users have some level of accountability.

a. Requirements. Each user organization is responsible for identifying its own functional common-user Information Management/Information Technology (IM/IT) business requirements to the Program Analysis and Integration Office (PAIO) for incorporation into the appropriate Installation Support Agreement. Each user organization must submit a detailed project or unique requirements to the DOIM, ATTN: IMSW-SMH-IMT-S. All IM/IT technical solutions must meet DOD, DA, HQ/MEDCOM, and installation standards or a waiver will be necessary. User organizations will forward waiver requests to the DOIM, ATTN: IMSW-SMH-IMT-S. The DOIM will review and verify all requests, risk assessments and the feasibility of the user organizations request. All waivers will be processed through the FSH IAM/CA and Designated Approval Authority (DAA).

b. Each organization shall appoint a primary and alternate Information Assurance Security Officer to coordinate Information Assurance activities with the DOIM Security Office.

c. User Training. It is the obligation of the user to request supervisor approval to attend training classes, seminars, educational assistance programs, etc., in order to increase their level of proficiency and to comply with appropriate directions.

d. User Assistance. Users will call the DOIM Help Desk (221-HELP) for IT assistance. Supervisors will discourage alternative, unofficial desktop support from non-DOIM personnel.

e. Equipment.

(1) Users, or unit/activity information assurance officer (IASO), will identify all IT installation, move, add, and change (IMAC) requirements to the DOIM. The IMACs of government equipment and equipment on lease will be done by DOIM to ensure correct technical configuration and asset management accuracy. Users or IASOs will provide sufficient notification (at least 10 work days) to DOIM in order to meet date, time, and location requirements.

(2) User, or unit IASO, will identify their functional requirements to DOIM for new leases, refresh or expiring leases, and new equipment purchases. Maximum lead-time (60-90 calendar days) will ensure DOIM meets customer requirements. Lease commitment is for a specified contract term; earlier termination is possible but must be coordinated with DOIM to identify final turn-in procedures and potential costs.

(3) Users are held accountable for the integrity, care, and property accountability of all IT equipment, both government-owned and leased.

(4) User or IASO will coordinate final disposal of IT equipment with DOIM.

(5) Users will leave all computers powered on after duty hours and will take no actions that interfere with information assurance scans, antivirus scans, or software updates being performed by automatic systems and/or DOIM staff.

f. Users of POC will request network accounts from the DOIM, ATTN: IMSW-SMH-IMT-S.

g. Each user is responsible for utilizing the computing equipment and network in accordance with the banner display at network or application logon, which is based upon higher headquarters' policy; the DOD Joint Ethics Regulation (Reference 1a); and as set forth in AR 25-1 and AR 25-2.

h. Information Structure resources:

(1) Users will only consume network file space and/or bandwidth for official government business, except as defined in reference 1f. The DOIM is authorized to enforce strict limits of network files space and purge excessive file folders to ensure availability and health of the network. Inappropriate or excessive use of bandwidth will be identified and reported to the Installation Commander.

(2) Users will not abuse the functionality of the Internet for non-business use (i.e, music videos, etc.). Violations will be reported to the Installation Commander.

(3) Users will not use government equipment to access material that is sexually oriented, demeans others, or that is of an extremist or terrorist nature (Reference 1e). The DOIM will maintain webfilters to limit/restrict access to unauthorized websites and resources. Suspected misuse will be referred to the Installation Commander for further action.

(4) Users will not abuse Email privileges. Users will perform regular housekeeping by purging or otherwise cleaning their Email accounts. The DOIM will enforce strict account limits and automatically purge excessive Email accounts to preserve the health and availability of Email resources. Users will not send chain letters, jokes, pornography, daily quotes, or unsubstantiated virus warnings in or attached to Email notes over the installation network. Reported violations will be reported to the Installation Commander for further action.

(5) Users and organizations are held accountable for misuse of network resources. Personal owned computers and devices are prohibited from the government owned network. Systems will be confiscate and investigated for possible compromise of government data. The system will be wiped with a government approved formatting tool prior to returning to the owner. The chain-of-command will take appropriate disciplinary actions.

(6) Users will immediately report suspected viruses to their units IASO and the DOIM Help Desk, 210-221-HELP.

(7) Users will not use government telecommunication services (telephones, cellular phones, pagers, radios, fax devices, etc.) for unofficial purposes, except as noted in Reference 1f.

(8) Incoming collect calls to official work sites are not permissible except in cases where the DOIM grants an exception for operational requirements.

(8) Personal long distance calls may be made from official work sites, if the user has first obtained the permission of his/her supervisor and the call is made at no expense to the Government. Government calling cards may only be used for official business.

(10) All tenant organizations will be responsible for respective costs of all telecommunications services incurred using telephone equipment, data circuits, excessive bandwidth, calling cards, cellular phones, pagers, or other special communications devices.

5. The policy will be reviewed 2 years from the implementation date.

6. The point of contact is Mr. Jack D. Poland, Director of Information Management, 221-1300/5281, or email address jack.poland1@us.army.mil.

RUSSELL J. CZERW
Major General, DC
Commanding

DISTRIBUTION:
A, B, Plus:
All Garrison Activities